

Appl. No. 10/534,855
Amendment A dated July 6, 2009
Reply to O.A. of February 3, 2009

PATENT
Docket No. 28944/40154

Remarks

Claims 45-85 are pending and at issue in the present application.

Claims 45-82 stand rejected under 35 U.S.C. § 101 for reciting a method that is not tied to a particular machine or that does not transform underlying subject matter to a different state or thing. Claim 45 has been amended to tie the method steps to the particular machine of a computer with a man/machine interface and an attacks/parries engine.

Further, claims 45-85 stand rejected under 35 U.S.C. § 112, ¶ 2, as being indefinite. The present amendment amends various claims to overcome the § 112 rejections noted by the examiner.

Still further, claims 45-85 stand rejected under 35 U.S.C. § 103 as obvious over various combinations of Sung et al., Apostol D. et al., Ritchey et al., Gupta et al., Dowd et al., Cohen et al., Pitchaikani et al., and Swiler et al. These rejections are respectfully traversed.

None of the applied references disclose or suggest a method or system, as recited by claims 45-85, that includes a modelling phase, comprising a specification of an architecture of an information system with a graphical representation of a set of components, wherein each component is associated with at least one state initialized with a sound value, wherein the at least one state corresponds to a security status of each component in the context of attacks launched against the information system, and wherein during a simulation phase, a successful attack causes a state of a component to pass to an unsound value.

Further, none of the applied references disclose or suggest a method or system, as recited by claims 45-85, that includes a modelling phase, comprising a specification of first and second sets of behavioural rules associated with a set of components of an information system, wherein the first set of behavioural rules is from the standpoint of an operation of the information system and the second set of behavioural rules is from the standpoint of security, and wherein each behavioural rule comprises at least one of one or more predicates and one or more actions.

The pending Office action states that "Sung teaches an intrusion model can be classified with four states, cool, warm, hot, and cool down" and identifies such "cool, warm, hot, and cool down" states as being analogous to a state associated with a component, as recited by the claims at issue. See Office action at page 2. However, such states are only cited by Sung in reference to another

Appl. No. 10/534,855
Amendment A dated July 6, 2009
Reply to O.A. of February 3, 2009

PATENT
Docket No. 28944/40154

prior art document, namely Wadlow. See Sung at page 322. More specifically, there is no support in Sung for combining the four states of Wadlow with any features of the method of Sung. Consequently, although Sung does disclose various states, e.g., cool, warm, hot, and cool down, Sung does not teach the initialization of such states with a sound value or a successful attack causing a state to pass to an unsound value, as recited by the claims at issue. Additionally, there is no disclosure or suggestion in Sung that the "cool, warm, hot, and cool down" states of Wadlow are analogous to the states recited by the claims at issue, which have been amended to clarify that such states relate to a security state of a component in the context of attacks launched against an information system.

Further, the examiner asserts that Sung discloses "phases," such as passive or busy, and identifies such phases as disclosing a state associated with a component, as recited by the claims at issue. See Office action at page 3. However, passive or busy states of a device have nothing to do with a security status of a component in the context of attacks launched against an information system, as recited by amended claims 45-85. Still further, the examiner asserts that "if a phase [of Sung] is not in the expected phase, it could be considered that an attack has altered the 'state' of the system and therefore the state is unsound or invalid." See Office action at page 3. The applicants respectfully disagree with this reasoning because there is no disclosure in Sung that changes in the passive or busy phases of devices are caused by attacks on the system and, as discussed above, passive and busy phases have nothing to do with a security state of a component, as recited by amended claims 45-85. Additionally, the examiner incorrectly identifies the component vulnerability disclosed in Sung as teaching the claimed unsound state. Indeed, as disclosed at the bottom of the page 327 of Sung, the component vulnerability is a performance index that is defined as a number of successful attacks divided by the total number of attempted attacks. This, again, has nothing to do with a state as claimed, which corresponds to a security status of a component at a given instant.

Further, as discussed in the Response dated December 5, 2008, and reiterated here, Apostol does not cure the deficiencies of Sung and, more specifically, does not disclose states relating to the vulnerability of a device based on a simulated attack. Likewise, none of the other applied references cures the above deficiencies of Sung and Apostol.

Appl. No. 10/534,855
Amendment A dated July 6, 2009
Reply to O.A. of February 3, 2009

PATENT
Docket No. 28944/40154

The applicants also respectfully traverse the assertion of the examiner that Sung discloses the first and second sets of behavioural rules, as recited by the claims at issue. Rather, chapter 3 of Sung teaches that network security simulation systems are organized within a set of layers that characterizes their design structure, as shown in Fig. 1 of Sung. This layered approach cannot be easily defined, based on the current understanding of the disclosure of this reference. What is clear, however, is that Sung fails to disclose first and second sets of behavioural rules associated with the components of the system, which each comprise at least one of one or more predicates and one or more actions as claimed. Further, none of the other applied references cures this deficiency of Sung.

For at least the foregoing reasons, reconsideration and withdrawal of the rejections of claims 45-85 and allowance of all the claims at issue are respectfully requested.

If there are any issues remaining that can be resolved by telephone, the examiner is invited to call the undersigned.

Deposit Account Authorization

The Commissioner is hereby authorized to charge any deficiency in any amount enclosed or any additional fees, which may be required during the pendency of this application under 37 CFR 1.16 or 1.17, except issue fees, to Deposit Account No. 50-1903.

Respectfully submitted,

MCCRACKEN & FRANK LLP
311 South Wacker Drive
Suite 2500
Chicago, IL 60606
(312) 263-4700
Customer No: 29471

July 6, 2009

By: 

Cato Yang
Reg. No. 57,310